UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,916	02/09/2004	Grigori M. Somin	30835/303181	1186

45373 7590 10/11/2007

MARSHALL, GERSTEIN & BORUN LLP (MICROSOFT)
233 SOUTH WACKER DRIVE
6300 SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	**PAPER NUMBER**
2139	

MAIL DATE	DELIVERY MODE
10/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

MN

Office Action Summary	Application No.	Applicant(s)	
	10/775,916	SOMIN ET AL.	
	Examiner	Art Unit	
	Benjamin A. Kaplan	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 12-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Response to communications filed on August 17, 2007

2. Claims 1-10 & 12-36 are rejected.

3. Claim 11 is canceled.

Claim Objections

4. Claim 35 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-10 & 12-35 are rejected under 35 U.S.C. 102(b) as being anticipated by Internet X.509 Public Key Infrastructure Certificate and CRL Profile. (RFC2459)

As Per Claim 1: RFC2459 teaches:

- A method for organizing and storing a peer identity in a peer-to-peer network by using an identity certificate data structure, the method comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 "Because a certificate's signature and timeliness can be independently checked by a certificate-using client, certificates can be distributed via untrusted communications and server systems, and can be cached in unsecured storage in certificate-using systems.").

- creating an identity public/private key pair comprising creating an identity public key and an identity private key

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 "The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate.").

- storing data representing the identity public key in a first data field of the identity certificate data structure

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- creating an identity peer name storing data representing the identity peer name in a second data field of the identity certificate data structure

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 "The identification may be based on either the key identifier (the subject key identifier in the issuer's certificate) or

on the issuer name and serial number.")

The Authority Key Identifier is the identity peer name.

- storing data representing a certificate type in a third data field of the identity certificate data structure the certificate type indicating an identity certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 "An object identifier is defined for the private extension.").

- creating a signature of the identity certificate, the signature derived, at least in part, from the identity private key

(Page 24 section 4.2.1.1 Authority Key Identifier first 3 lines "The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate.").

- storing data representing the signature of the identity certificate in a fourth data field of the identity certificate data structure

(Page 17 section 4.1.2.3 Signature paragraph 1 "This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate.").

As Per Claim 2: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- using the identity certificate data structure comprises using an X.509 certificate

A X.509 certificate as seen in the rejection of claim 1 is inherently a X.509 certificate.

As Per Claim 3: The rejection of claim 2 is incorporated and further RFC2459 teaches:

- storing data representing the identity peer name in the second data field comprises storing data representing the identity peer name in a subject alternative name field of the X.509 certificate

(Page 24 section 4.2.1.1 Authority Key Identifier first paragraph lines 3-7 "This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification may be based on either the key identifier (the subject key identifier in the issuer's certificate) or on the issuer name and serial number.").

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 "The subject alternative names extension allows additional identities to be bound to the subject of the certificate.").

As Per Claim 4: The rejection of claim 2 is incorporated and further RFC2459 teaches:

- storing data representing a certificate type in the third data field comprises storing data representing a certificate type in an extension property field of the X.509 certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 "An object

identifier is defined for the private extension.").

As Per Claim 5: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- creating the identity peer name comprises creating a globally unique identity peer name

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 "The value of the keyIdentifier field SHOULD be derived from the public key used to verify the certificate's signature or a method that generates unique values.").

As Per Claim 6: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- creating the identity peer name comprises deriving the identity peer name from, at least in part, the identity public key

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5).

As Per Claim 7: The rejection of claim 6 is incorporated and further RFC2459 teaches:

- deriving the identity peer name from, at least in part, the identity public key comprises deriving the identity peer name from, at least in part, a hash of the identity public key

(Page 24 section 4.2.1.2 Subject Key Identifier paragraph 2 lines 4-7 "The value of the subject key identifier MUST be the value placed in the key identifier field of the Authority Key Identifier extension (see sec. 4.2.1.1) of certificates issued by the subject of this certificate.").

(Section 4.2.1.2 Subject Key Identifier page 25 paragraph 2 "(1) The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).").

As Per Claim 8: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- storing data representing the identity private key in a secure container and storing a reference to the data representing the identity private key in association with the identity certificate data structure

(Section 3.5 Management Protocols Page 13 subsection (d) lines 1-3 "key pair recovery: As an option, user client key materials (e.g., a user's private key used for encryption purposes) may be backed up by a CA or a key backup system.").

The key backup system is the secure container. References are inherent in the use of stored data.

As Per Claim 9: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- storing user identification data in at least one of a fifth and a sixth data field of the identity certificate data structure, the user identification data representing a user at whose request the peer identity was created

(Page 17 section 4.1.2.4 Issuer lines 1-2 "The issuer field identifies the entity who has signed and issued the certificate.").

(Page 21 section 4.1.2.6 Subject lines 1-2 "The subject field identifies the entity associated with the public key stored in the subject public key field.").

(Page 21 section 4.1.2.6 Subject lines 3-8 "If the subject is a CA (e.g., the basic constraints extension, as discussed in 4.2.1.10, is present and the value of cA is TRUE,) then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field (see sec. 4.1.2.4) in all certificates issued by the subject CA.").

As Per Claim 10: The rejection of claim 1 is incorporated and further RFC2459 teaches:

- at least one of: storing data representing a period of validity of the identity certificate in a seventh data field of the identity certificate data structure; and storing data representing a version of the identity certificate in an eighth data field of the identity certificate data structure.

(Page 20 section 4.1.2.5 Validity lines 1-3 "The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates:").

(Page 16 section 4.1.2.1 Version line 1 "This field describes the version of the encoded certificate.").

As Per Claim 12: RFC2459 teaches:

- A method for organizing and storing a group identity in a peer-to-peer network by using a group root certificate data structure, the method comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 as seen in the rejection of claim 1.).

(Page 9 section 3.2 Certification Paths and Trust paragraph 3 lines 1-3 "Internet Policy Registration Authority (IPRA): This authority, operated under the auspices of the Internet Society, acts as the root of the PEM certification hierarchy at level 1.").

A root X.509 certificate is this certificate.

- creating a group root public/private key pair comprising creating a group root public key and a group root private key; storing data representing the group root public key in a first data field of the, group root certificate data structure

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 as seen in the rejection of claim 1).

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- creating a group peer name; storing data representing the group peer name in a second data field of the group root certificate data structure

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- storing data representing a certificate type in a third data field of the group root certificate data structure, the certificate type indicating a group root certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- creating a signature of the group root certificate, the signature derived, at least in part, from the group root private key; and storing data representing the signature of the group root certificate in a fourth data field of the group root certificate data structure

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

(Page 24 section 4.2.1.1 Authority Key Identifier first 3 lines as seen in the rejection of claim 1.).

As Per Claim 13: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- using the group root certificate data structure comprises using an X.509 certificate

A X.509 certificate as seen in the rejection of claim 12 is inherently a X.509 certificate.

As Per Claim 14: The rejection of claim 13 is incorporated and further RFC2459 teaches:

- storing data representing the group peer name in the second data field comprises storing data representing the group peer name in a subject alternative name field of the X.509 certificate

(Page 24 section 4.2.1.1 Authority Key Identifier first paragraph lines 3-7 as seen in the rejection of claim 3.).

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 as seen in the rejection of claim 3.).

As Per Claim 15: The rejection of claim 13 is incorporated and further RFC2459 teaches:

- storing data representing the certificate type in the third data field comprises storing data representing the certificate type in an extension property field of the X.509 certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 4).

As Per Claim 16: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- creating the group peer name comprises creating a is globally unique group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5.).

As Per Claim 17: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- creating the group peer name comprises deriving the group peer name, at least in part, from the group root public key

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5.).

As Per Claim 18: The rejection of claim 17 is incorporated and further RFC2459 teaches:

- deriving the group peer name, at least in part, from the group root public key comprises deriving the group peer name, at least in part, from a hash of the group root public key

(Page 24 section 4.2.1.2 Subject Key Identifier paragraph 2 lines 4-7 as seen in the rejection of claim 7.).

(Section 4.2.1.2 Subject Key Identifier page 25 paragraph 2 as seen in the rejection of claim 7.).

As Per Claim 19: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- storing user identification data in at least one of a fifth and a sixth data field of the group root certificate data structure, the user identification data representing a user at whose request the group identity was created

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

(Page 21 section 4.1.2.6 Subject lines 1-2 as seen in the rejection of claim 9.).

(Page 21 section 4.1.2.6 Subject lines 3-8 as seen in the rejection of claim 9.).

As Per Claim 20: The rejection of claim 12 is incorporated and further RFC2459

teaches:

- storing data representing a period of validity of the group root certificate in a seventh data field of the group root certificate data structure

(Page 20 section 4.1.2.5 Validity lines 1-3 as seen in the rejection of claim 10.).

As Per Claim 21: The rejection of claim 12 is incorporated and further RFC2459 teaches:

- storing data representing a version of the group root certificate in an eighth data field of the group root certificate data structure

(Page 16 section 4.1.2.1 Version line 1 as seen in the rejection of claim 11.).

As Per Claim 22: RFC2459 teaches:

- A method for organizing and storing a group membership identity corresponding to a group identity and a group member in a peer-to-peer network using a group membership certificate data structure, the method comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 as seen in the rejection of claim 1.).

(Page 10 line 17-19 "CAs represent, for example, particular organizations, particular organizational units (e.g., departments, groups, sections), or particular geographical

areas.")

A group level X.509 certificate is this certificate. The certificate can be cached showing a computer readable medium.

- storing data representing a group peer name in a first data field of the group membership certificate data structure, wherein the ,group peer name corresponds to a group peer name of the group identity

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- storing data representing an issuer peer name in a second data field of the group membership certificate data structure

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

- storing data representing a subject peer name in a third data field of the group membership certificate data structure, the subject peer name comprising a reference to a peer identity certificate of the group member

(Page 21 section 4.1.2.6 Subject lines 1-2 as seen in the rejection of claim 9.).

- storing data representing a certificate type in a fourth data field of the group membership certificate data structure, the certificate type indicating a group membership certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- storing data representing a signature of the group membership certificate in a fifth data field of the group membership certificate data structure

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

As Per Claim 23: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- using the group membership certificate data structure comprises using an X.509 certificate

A X.509 certificate as seen in the rejection of claim 22 is inherently a X.509 certificate.

As Per Claim 24: The rejection of claim 23 is incorporated and further RFC2459 teaches:

- storing data representing a group peer name in the first data field comprises storing data representing a group peer name in an extension property field of the X.509 certificate

(Page 24 section 4.2.1.1 Authority Key Identifier first paragraph lines 3-7 as seen in the rejection of claim 3.).

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 as seen in the rejection of claim 3.).

As Per Claim 25: The rejection of claim 23 is incorporated and further RFC2459 teaches:

- storing data representing an issuer peer name in the second data field comprises storing data representing an issuer peer name in an issuer alternative name field of the X.509 certificate

(Page 32 section 4.2.1.8 Issuer Alternative Names lines 1-3 "As with 4.2.1.7, this extension is used to associate Internet style identities with the certificate issuer. Issuer alternative names MUST be encoded as in 4.2.1.7.").

As Per Claim 26: The rejection of claim 23 is incorporated and further RFC2459 teaches:

- storing data representing a subject peer name in the third data field comprises storing data representing a subject peer name in a subject alternative name field of the X.509 certificate

(Page 30 section 4.2.1.7 Subject Alternative Name lines 1-2 as seen in the rejection of claim 3.).

As Per Claim 27: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- storing data representing the group peer name in the first data field comprises storing data representing a globally unique group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5.).

As Per Claim 28: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- storing data representing the issuer peer name in the second data field comprises storing data representing a reference to a certificate selected from the group consisting of: a group root certificate corresponding to the group identity and a neighbor group membership certificate corresponding to a neighbor group member

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.)

It is inherent that since the issuer field identifies the entity that issued a certificate the issuing entity will be referred to in this field, as such any entity that can issue a certificate would be in the group of possible entries for this field.

As Per Claim 29: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- storing data representing a period of validity of the group membership certificate in a sixth data field of the group membership certificate data structure

(Page 20 section 4.1.2.5 Validity lines 1-3 as seen in the rejection of claim 10.).

As Per Claim 30: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- storing data representing a version of the group membership certificate in a seventh data field of the group membership certificate data structure

(Page 16 section 4.1.2.1 Version line 1 as seen in the rejection of claim 11.).

As Per Claim 31: The rejection of claim 22 is incorporated and further RFC2459 teaches:

- creating a signature of the group membership certificate, comprising: if the group root private key is known, deriving the signature, at least in part, from a group root private key corresponding to the ,group root certificate; and if the group root private key is unknown, deriving the signature, at least in part, from a group membership private key of a created group membership public/ private key pair

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1).

(Page 24 section 4.2.1.1 Authority Key Identifier first 3 lines as seen in the rejection of claim 1).

(Page 24 section 4.2.1.1 Authority Key Identifier paragraph 3 lines 1-3 as seen in the rejection of claim 5).

As Per Claim 32: RFC2459 teaches:

- A method for organizing a group identity store for use in a peer-to-peer network by using a group certificate chain data structure, the method comprising:

(Page 8 section 3.1 X.509 Version 3 Certificate first paragraph lines 11-15 as seen in the rejection of claim 1.).

(Page 9 section 3.2 Certification Paths and Trust lines 7-8 "In general, a chain of multiple certificates may be needed,").

A X.509 certificate path or chain of certificates is this chain data structure. The certificates can be cached showing a computer readable medium.

- storing in a first portion of the group certificate chain data structure data representing a group root certificate created per a request of a user comprising:

(Page 9 section 3.2 Certification Paths and Trust paragraph 3 lines 1-3 as seen in the rejection of claim 12).

(Document title X.509 Public Key Infrastructure Certificate and CRL Profile).

A root X.509 certificate is this certificate.

- storing data representing a group peer name corresponding to the group root certificate

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- storing data representing a group root public key corresponding to the group root certificate

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- storing data representing a certificate type, the certificate type indicating the group root certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- storing data representing a signature of the group root certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

- the signature derived, at least in part, from a group root private key

(Page 24 section 4.2.1.1 Authority Key Identifier first 3 lines as seen in the rejection of claim 1.).

- the group root private key and the group root public key forming a public/private key pair

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 as seen in the rejection of claim 1).

- storing in a second portion of the group certificate chain data structure data representing a group membership certificate corresponding to the group root certificate comprising:

(Document title X.509 Public Key Infrastructure Certificate and CRL Profile)

(Page 10 line 17-19 as seen in the rejection of claim 22)

A group level X.509 certificate issued from the root certificate authority is this certificate.

- storing data representing the group peer name

(Page 24 section 4.2.1.1 Authority Key Identifier lines 5-7 as seen in the rejection of claim 1.).

The Authority Key Identifier is the group peer name.

- storing data representing an issuer peer name

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

- the issuer peer name comprising a reference to the group root certificate

(Page 17 section 4.1.2.4 Issuer lines 1-2 as seen in the rejection of claim 9.).

It is inherent that since the issuer field identifies the entity that issued a certificate and the root certificate issued this certificate the root certificate would be referred to as the issuer.

- storing data representing a subject peer name

(Page 21 section 4.1.2.6 Subject lines 1-2 as seen in the rejection of claim 9.).

- storing data representing a certificate type, the certificate type indicating the group membership certificate

(Page 38 section 4.2.2 Private Internet Extensions paragraph 2 line 1 as seen in the rejection of claim 1).

- storing data representing a signature of the group membership certificate

(Page 17 section 4.1.2.3 Signature paragraph 1 as seen in the rejection of claim 1.).

As Per Claim 33: The rejection of claim 32 is incorporated and further RFC2459 teaches:

- storing data representing the group root certificate and storing data representing the group membership certificate comprise storing X.509 certificates

X.509 certificates as seen in the rejection of claim 32 are inherently X.509 certificates.

As Per Claim 34: The rejection of claim 32 is incorporated and further RFC2459 teaches:

- storing data representing a member public key

(Page 22 section 4.1.2.7 Subject Public Key Info line 1 "This field is used to carry the public key").

- the member public key and a member private key forming a member public/private key pair

(Page 24 section 4.2.1.1 Authority Key Identifier lines 1-3 as seen in the rejection of claim 1).

As Per Claim 35: The limitations of claim 35 are redundant to the limitations of claims 32 & 34.

7. Claim 36 is rejected under 35 U.S.C. 102(b) as being anticipated by keytool - Key and Certificate Management Tool. (Sun)

As Per Claim 36: Sun teaches:

- A method for organizing a peer identity store for use in a peer-to-peer network comprising:

identifying a set of one or more identity certificates created per request of a user, collecting the set of one or more identity certificates into the peer identity store, and setting a profile of the user to refer to the peer identity store.

(Page 1, Lines 1-3, "Manages a keystore (database) of private keys and their associated X.509 certificate chains authenticating the corresponding public keys. Also manages certificates from trusted entities.").

(Pages 2-3, Section Keystore Location, "Each keytool command has a -keystore option for specifying the name and location of the persistent keystore file for the keystore managed by keytool. The keystore is by default stored in a file named .keystore in the

user's home directory, as determined by the "user.home" system property. Given user name uName, the "user.home" property value defaults to

C:\Winnt\Profiles\uName on multi-user Windows NT systems

C:\Windows\Profiles\uName on multi-user Windows 95 systems

C:\Windows on single-user Windows 95 systems

Thus, if the user name is "cathy", "user.home" defaults to

C:\Winnt\Profiles\cathy on multi-user Windows NT systems

C:\Windows\Profiles\cathy on multi-user Windows 95 systems").

Response to Amendment and Arguments

Restating claims of structures that were not patentably distinct from the X.509 certificate standard structures as methods that are performing the same functions does not render the claims distinct from the X.509 standard.

That the claimed invention is not in all claims necessarily a X.509 certificate in does not reduce the teachings of the X.509 standard.

The intended use of an invention is not a limitation of the claimed invention. Additionally the use of X.509 certificates in peer-to-peer environments was also well know in the art at the time of invention was made (e.g. provided excerpt from PGP Freeware for Windows 95, Windows 98, Windows NT, Windows 2000 & Windows Millennium User's Guide version 7.0)

The rejections of claims 1-35 under 35 USC § 101 have been withdrawn.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin A. Kaplan whose telephone number is 571-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100